PCT/JP2004/008653

14. 6. 2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　６月１２日

出願番号
Application Number: 特願２００３－１６７３７４
[ST. 10/C]: [ＪＰ２００３－１６７３７４]

出願人
Applicant(s): 松下電器産業株式会社

２００４年　７月１４日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３０６１０６

【書類名】　特許願
【整理番号】　2022550095
【提出日】　平成15年 6月12日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C　5/00
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　布田　裕一
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　山道　将人
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　大森　基司
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　館林　誠
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100090446
【弁理士】
【氏名又は名称】　中島　司朗

【手数料の表示】

【予納台帳番号】　014823

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9003742

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号通信システム

【特許請求の範囲】

【請求項１】　メッセージを秘密に通信する暗号通信システムであって、

１個のメッセージを記憶している記憶手段と、

前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成する暗号手段と、

前記メッセージに一方向性演算を施して比較演算値を生成する演算手段と、

生成した前記複数の暗号文と前記比較演算値とを送信する送信手段と

を備える暗号送信装置と、

前記複数の暗号文と前記比較演算値とを受信する受信手段と、

前記複数の暗号文の各々に対して、前記暗号化演算に対応する復号演算により同数の復号メッセージを生成する復号手段と、

前記複数の復号メッセージの各々に、前記一方向性演算を施して、同数の復号演算値を生成する演算手段と、

生成した各復号演算値と受信した前記比較演算値とを比較して、少なくとも１組の前記復号演算値と前記比較演算値とが一致すれば、前記メッセージの正当な復号文として、当該組に対応する復号メッセージを出力し、全ての組の前記復号演算値と前記比較演算値とが不一致であれば、復号エラーを出力する判定手段と

を備える暗号受信装置と

から構成されることを特徴とする暗号通信システム。

【請求項２】　前記暗号手段は、ＮＴＲＵ暗号による暗号化演算により暗号文を生成し、

前記復号手段は、ＮＴＲＵ暗号による復号演算により復号メッセージを生成する

ことを特徴とする請求項１に記載の暗号通信システム。

【請求項３】　メッセージを秘密に送信する暗号送信装置であって、

１個のメッセージを記憶している記憶手段と、

前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成

する暗号手段と、

前記メッセージに一方向性演算を施して比較演算値を生成する演算手段と、

生成した前記複数の暗号文と前記比較演算値とを送信する送信手段と

を備えることを特徴とする暗号送信装置。

【請求項４】　前記暗号手段は、

前記メッセージに対して、可逆のデータ変換を施して、変換メッセージを生成し、生成した変換メッセージに対して、暗号アルゴリズムを施して暗号文を生成する前記暗号化演算を行う暗号化演算部と、

前記暗号化演算部に対して、変換メッセージの生成と暗号文の生成とを前記複数回繰り返すように制御する繰返制御部と

を含むことを特徴とする請求項３に記載の暗号送信装置。

【請求項５】　前記暗号化演算部は、固定長の乱数を生成し、前記メッセージに対して、生成した前記乱数を付加することにより、前記変換メッセージを生成する

ことを特徴とする請求項４に記載の暗号送信装置。

【請求項６】　前記暗号化演算部は、ＮＴＲＵ暗号による暗号アルゴリズムにより暗号文を生成する

ことを特徴とする請求項５に記載の暗号送信装置。

【請求項７】　暗号送信装置からメッセージを秘密に受信する暗号受信装置であって、

前記暗号送信装置は、１個のメッセージを記憶しており、前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成し、前記メッセージに一方向性演算を施して比較演算値を生成し、生成した前記複数の暗号文と前記比較演算値とを送信し、

前記暗号受信装置は、

前記複数の暗号文と前記比較演算値とを受信する受信手段と、

前記複数の暗号文の各々に対して、前記暗号化演算に対応する復号演算により同数の復号メッセージを生成する復号手段と、

前記複数の復号メッセージの各々に、前記一方向性演算を施して、同数の復号

演算値を生成する演算手段と、

生成した各復号演算値と受信した前記比較演算値とを比較して、少なくとも１組の前記復号演算値と前記比較演算値とが一致すれば、前記メッセージの正当な復号文として、当該組に対応する復号メッセージを出力し、全ての組の前記復号演算値と前記比較演算値とが不一致であれば、復号エラーを出力する判定手段と

を備えることを特徴とする暗号受信装置。

【請求項８】　前記暗号送信装置は、前記メッセージに対して、可逆のデータ変換を施して、変換メッセージを生成し、生成した変換メッセージに対して、暗号アルゴリズムを施して暗号文を生成する前記暗号化演算を行い、変換メッセージの生成と暗号文の生成とを前記複数回繰り返し、

前記復号手段は、

前記暗号文に対して、前記暗号アルゴリズムに対応する復号アルゴリズムを施して復号文を生成し、生成した復号文に対して、前記データ変換の逆変換を施して、復号メッセージを生成する前記復号演算を行う復号演算部と、

前記復号演算部とに対して、復号文の生成と復号メッセージの生成とを、前記複数回繰り返すように制御する繰返制御部と

を含むことを特徴とする請求項７に記載の暗号受信装置。

【請求項９】　前記暗号送信装置は、固定長の乱数を生成し、前記メッセージに対して、生成した前記乱数を付加することにより、前記変換メッセージを生成し、

前記復号演算部は、生成した復号文から、前記固定長の乱数部分を除去して復号メッセージを生成する

ことを特徴とする請求項８に記載の暗号受信装置。

【請求項１０】　暗号送信装置は、ＮＴＲＵ暗号による暗号アルゴリズムにより暗号文を生成し、

前記復号演算部は、ＮＴＲＵ暗号による復号アルゴリズムにより復号文を生成する

ことを特徴とする請求項９に記載の暗号受信装置。

【請求項１１】　１個のメッセージを記憶している記憶手段を備え、前記メッ

セージを秘密に送信する暗号送信装置で用いられる暗号送信方法であって、

前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成する暗号ステップと、

前記メッセージに一方向性演算を施して比較演算値を生成する演算ステップと、

生成した前記複数の暗号文と前記比較演算値とを送信する送信ステップと

を含むことを特徴とする暗号送信方法。

【請求項１２】　１個のメッセージを記憶している記憶手段を備え、前記メッセージを秘密に送信する暗号送信装置で用いられる暗号送信プログラムであって、

前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成する暗号ステップと、

前記メッセージに一方向性演算を施して比較演算値を生成する演算ステップと、

生成した前記複数の暗号文と前記比較演算値とを送信する送信ステップと

を含むことを特徴とする暗号送信プログラム。

【請求項１３】　コンピュータ読み取り可能な記録媒体に記録されている

ことを特徴とする請求項１２に記載の暗号送信プログラム。

【請求項１４】　暗号送信装置からメッセージを秘密に受信する暗号受信装置で用いられる暗号受信方法であって、

前記暗号送信装置は、１個のメッセージを記憶しており、前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成し、前記メッセージに一方向性演算を施して比較演算値を生成し、生成した前記複数の暗号文と前記比較演算値とを送信し、

前記暗号受信方法は、

前記複数の暗号文と前記比較演算値とを受信する受信ステップと、

前記複数の暗号文の各々に対して、前記暗号化演算に対応する復号演算により同数の復号メッセージを生成する復号ステップと、

前記複数の復号メッセージの各々に、前記一方向性演算を施して、同数の復号

演算値を生成する演算ステップと、

生成した各復号演算値と受信した前記比較演算値とを比較して、少なくとも１組の前記復号演算値と前記比較演算値とが一致すれば、前記メッセージの正当な復号文として、当該組に対応する復号メッセージを出力し、全ての組の前記復号演算値と前記比較演算値とが不一致であれば、復号エラーを出力する判定ステップと

を含むことを特徴とする暗号受信方法。

【請求項１５】　暗号送信装置からメッセージを秘密に受信する暗号受信装置で用いられる暗号受信プログラムであって、

前記暗号送信装置は、１個のメッセージを記憶しており、前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成し、前記メッセージに一方向性演算を施して比較演算値を生成し、生成した前記複数の暗号文と前記比較演算値とを送信し、

前記暗号受信プログラムは、

前記複数の暗号文と前記比較演算値とを受信する受信ステップと、

前記複数の暗号文の各々に対して、前記暗号化演算に対応する復号演算により同数の復号メッセージを生成する復号ステップと、

前記複数の復号メッセージの各々に、前記一方向性演算を施して、同数の復号演算値を生成する演算ステップと、

生成した各復号演算値と受信した前記比較演算値とを比較して、少なくとも１組の前記復号演算値と前記比較演算値とが一致すれば、前記メッセージの正当な復号文として、当該組に対応する復号メッセージを出力し、全ての組の前記復号演算値と前記比較演算値とが不一致であれば、復号エラーを出力する判定ステップと

を含むことを特徴とする暗号受信プログラム。

【請求項１６】　コンピュータ読み取り可能な記録媒体に記録されている

ことを特徴とする請求項１５に記載の暗号受信プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報セキュリティ技術としての暗号技術に関する。

【０００２】

【従来の技術】

近年、家庭用電化製品で使用されるような比較的処理能力の低いプロセッサであっても、実装可能なＮＴＲＵ暗号が注目されている。

ＮＴＲＵ暗号では、多項式演算（加算及び乗算）が基本演算であり、多項式の各係数は、８ビット以下である。このため、８ビットＣＰＵでもＮＴＲＵ暗号が容易に実装できる。ＮＴＲＵ暗号は、楕円曲線暗号と比較して１０～５０倍高速であり、また、楕円曲線暗号で必要な多倍長ライブラリが不要であるので、コードサイズが楕円曲線暗号と比較して小さいという利点がある。なお、ＮＴＲＵ暗号については、非特許文献１及び特許文献１により開示されているので、説明を省略する。

【０００３】

しかし、ＮＴＲＵ暗号では、復号時にエラーが発生する可能性があり、復号時に、このエラーの検出ができないので、復号が正しく行われたか否かの保証ができないという問題点がある。

この問題点を解決するために、特許文献２によると、送信装置は、平文に一方向性関数を施して第１関数値を生成し、第１付加情報を生成し、前記平文及び前記第１付加情報に可逆演算を施して、結合情報を生成し、前記結合情報に暗号アルゴリズムを施して暗号文を生成する。受信装置は、第１付加情報と同一の第２付加情報を生成し、前記暗号文に、復号アルゴリズムを施して復号結合情報を生成し、前記復号結合情報及び第２付加情報に前記可逆演算の逆演算を施して、復号文を生成し、復号された復号文に前記一方向性関数を施して第２関数値を生成し、前記第１関数値と前記第２関数値とを比較し、一致する場合に復号文が正当であると判断する。このようにして、平文が正しく復号できたか否かを判断することができる。

【０００４】

平文が正しく復号できなかったと判断される場合には、受信側は、送信側に対

して、再度、暗号文を送信するように要求し、再度暗号文を受信すればよい。

【０００５】

【非特許文献１】

Jeffrey Hoffstein, Jill Pipher and Joseph H.Silverman, "NTRU:A ring based public key cryptosystem",Lecture Notes in Computer Science, 1423, pp.267-288, Springer-Verlag,1998

【０００６】

【特許文献１】

米国特許番号6,081,597

【０００７】

【特許文献２】

特開2002-252611号公報

【０００８】

【非特許文献２】

J. Proos, "Imperfect Decryption and an Attack on the NTRU Encryption Scheme", IACR ePrint Archive, 2003/002, http://eprint.iacr.org/, (2003).

【０００９】

【発明が解決しようとする課題】

しかしながら、非特許文献２によると、ＮＴＲＵ暗号において、攻撃者が受信者に対して適当なデータを送信し、再送要求が起こるか否かをチェックすることにより、鍵を求める攻撃方法が開示されている。このためＮＴＲＵ暗号を使用する場合において、安全性を確保できないという問題点がある。

【００１０】

本発明は、暗号方式において、再送要求による攻撃を回避することができる暗号通信システム、暗号送信装置、暗号送信方法、暗号送信プログラム、暗号受信装置、暗号受信方法及び暗号受信プログラムを提供することを目的とする。

【００１１】

【課題を解決するための手段】

上記目的を達成するために、暗号送信装置は、送信する１個のメッセージを５

回暗号化して５個の暗号化メッセージを生成し、メッセージのハッシュ値を算出し、５個の暗号化メッセージとハッシュ値とを送信する。暗号受信装置は、５個の暗号化メッセージとハッシュ値とを受信し、５個の暗号化メッセージを復号してそれぞれ復号メッセージを生成し、生成した復号メッセージの復号ハッシュ値をそれぞれ算出し、算出した復号ハッシュ値と受信したハッシュ値とを比較する。１組でも一致すれば、対応する復号メッセージを正しいものとみなす。５組の全てで一致しなければ、復号エラーとみなす。

【００１２】

【発明の実施の形態】

本発明に係る１個の実施の形態としての映像再生システム１０について説明する。

１．映像再生システム１０

映像再生システム１０は、図１に示すように、サーバ装置１００と映像再生装置２００とから構成されており、サーバ装置１００と映像再生装置２００とは、インターネット２０を介して接続されている。

【００１３】

サーバ装置１００は、コンテンツを暗号化し、暗号化コンテンツをインターネット２０を介して、映像再生装置２００へ送信する。映像再生装置２００は、暗号化コンテンツを受信し、受信した暗号化コンテンツを復号してコンテンツを生成し、生成したコンテンツを再生し、映像再生装置２００に接続されているモニタ５０及びスピーカ４０へ映像及び音声を出力する。

【００１４】

１．１　サーバ装置１００の構成

サーバ装置１００は、図２に示すように、情報記憶部１０１、乱数生成部１０２、第１暗号化部１０３、ハッシュ部１０４、第２暗号化部１０５、送受信部１０６、制御部１０７、入力部１０８及び表示部１０９から構成されている。

サーバ装置１００は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニ

ットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、サーバ装置１００は、その一部の機能を達成する。

【００１５】

（１）情報記憶部１０１

情報記憶部１０１は、図２に示すように、公開鍵Ｋｐ、コンテンツ鍵Ｋｃ及びコンテンツＣを記憶している。

公開鍵Ｋｐは、ＮＴＲＵ暗号の鍵生成方法により生成された秘密鍵Ｋｓ（後述する）を元にして生成された公開鍵であり、２６３次元のＮＴＲＵ暗号の場合に、１８４１ビット長である。

【００１６】

また、コンテンツ鍵Ｋｃは、１６８ビットの鍵であり、コンテンツＣを暗号化する際に用いられる。

また、コンテンツＣは、映像情報及び音声情報から構成される映画データである。

（２）乱数生成部１０２

乱数生成部１０２は、制御部１０７の制御の基に、６４ビットの乱数Ｒｉの生成及び生成した乱数Ｒｉの第１暗号化部１０３への出力を、５回繰り返す。

【００１７】

（３）第１暗号化部１０３

第１暗号化部１０３は、制御部１０７の制御の基に、情報記憶部１０１から公開鍵Ｋｐ及びコンテンツ鍵Ｋｃを読み出す。次に、第１暗号化部１０３は、制御部１０７の制御の基に、以下の処理（ａ）～（ｃ）を５回繰り返す。

（ａ）乱数生成部１０２から乱数Ｒｉを受け取る。

【００１８】

（ｂ）読み出したコンテンツ鍵Ｋｃ及び受け取った乱数Ｒｉを結合する。

Ｋｃ｜｜Ｒｉ

（ｃ）公開鍵Ｋｐを用いて、コンテンツ鍵Ｋｃ及び乱数Ｒｉの結合に対して、暗号化アルゴリズムＥｎｃ１を施して、暗号化コンテンツ鍵ＥＫｃｉを生成する

。

【００１９】

ＥＫｃｉ＝Ｅｎｃ１（Ｋｐ、Ｋｃ｜｜Ｒｉ）

ここで、「｜｜」は、結合を示す演算子であり、暗号化アルゴリズムＥｎｃ１は、ＮＴＲＵ暗号によるアルゴリズムであり、Ｘ＝Ｅｎｃ１（Ｙ、Ｚ）は、鍵Ｙを用いて、平文Ｚに対して暗号化アルゴリズムＥｎｃ１を施して暗号文Ｘを得ることを示す。

【００２０】

こうして、５個の暗号化コンテンツ鍵ＥＫｃ１、ＥＫｃ２、・・・、ＥＫｃ５が生成される。

次に、第１暗号化部１０３は、生成した５個の暗号化コンテンツ鍵ＥＫｃ１、ＥＫｃ２、・・・、ＥＫｃ５を送受信部１０６へ出力する。

なお、図２において、各ブロックは、接続線により他のブロックと接続されている。ただし、一部の接続線を省略している。ここで、各接続線は、信号や情報が伝達される経路を示している。また、第１暗号化部１０３を示すブロックに接続している複数の接続線のうち、接続線上に鍵マークが付されているものは、第１暗号化部１０３へ鍵としての情報が伝達される経路を示している。第２暗号化部１０５を示すブロックについても同様である。また、他の図面についても同様である。

【００２１】

（４）ハッシュ部１０４

ハッシュ部１０４は、制御部１０７の制御の基に、情報記憶部１０１からコンテンツ鍵Ｋｃを読み出し、読み出したコンテンツ鍵Ｋｃに対して、一方向性関数であるハッシュ関数Ｈａｓｈを施して、ハッシュ値Ｈを生成する。

Ｈ＝Ｈａｓｈ（Ｋｃ）

ここで、ハッシュ関数Ｈａｓｈの一例は、ＳＨＡ－１である。なお、ＳＨＡ－１については、公知であるので、説明を省略する。この場合に、ハッシュ値Ｈは、１６０ビット長である。

【００２２】

次に、ハッシュ部１０４は、生成したハッシュ値Ｈを送受信部１０６へ出力する。

（５）第２暗号化部１０５

第２暗号化部１０５は、制御部１０７の制御の基に、情報記憶部１０１からコンテンツ鍵Ｋｃ及びコンテンツＣを読み出し、読み出したコンテンツ鍵Ｋｃを用いて、読み出したコンテンツＣに暗号化アルゴリズムＥｎｃ２を施して、暗号化コンテンツＥＣを生成する。

【００２３】

ＥＣ＝Ｅｎｃ２（Ｋｃ、Ｃ）

ここで、暗号化アルゴリズムＥｎｃ２は、トリプルＤＥＳによるアルゴリズムである。なお、トリプルＤＥＳについては、公知であるので、説明を省略する。

次に、第２暗号化部１０５は、生成した暗号化コンテンツＥＣを送受信部１０６へ出力する。

【００２４】

（６）送受信部１０６

送受信部１０６は、インターネット２０を介して、映像再生装置２００と接続されている。

送受信部１０６は、制御部１０７の制御の基に、第１暗号化部１０３から５個の暗号化コンテンツ鍵ＥＫｃ１、ＥＫｃ２、・・・、ＥＫｃ５を受け取り、ハッシュ部１０４からハッシュ値Ｈを受け取り、第２暗号化部１０５から暗号化コンテンツＥＣを受け取り、受け取った５個の暗号化コンテンツ鍵ＥＫｃ１、ＥＫｃ２、・・・、ＥＫｃ５、ハッシュ値Ｈ及び暗号化コンテンツＥＣを、インターネット２０を介して、映像再生装置２００へ送信する。

【００２５】

（７）制御部１０７、入力部１０８及び表示部１０９

制御部１０７は、乱数生成部１０２、第１暗号化部１０３、ハッシュ部１０４、第２暗号化部１０５及び送受信部１０６を制御する。

入力部１０８は、サーバ装置１００の操作者から操作指示を受け付け、受け付けた指示を制御部１０７へ出力する。

【００２６】

表示部１０９は、制御部１０７の制御の基に、各種の情報を表示する。

１．２　映像再生装置２００の構成

映像再生装置２００は、図３に示すように、送受信部２０１、第１復号部２０２、ハッシュ部２０３、判定部２０４、情報記憶部２０５、第２復号部２０６、再生部２０７、制御部２０８、入力部２０９及び表示部２１０から構成されている。

【００２７】

映像再生装置２００は、サーバ装置１００と同様に、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを含んで構成される。前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、映像再生装置２００は、その一部の機能を達成する。

【００２８】

（１）情報記憶部２０５

情報記憶部２０５は、図３に示すように、秘密鍵Ｋｓを記憶している。

秘密鍵Ｋｓは、ＮＴＲＵ暗号の鍵生成方法により生成された秘密鍵であり、２６３次元のＮＴＲＵ暗号の場合には、４１５ビット長である。

（２）送受信部２０１

送受信部２０１は、インターネット２０を介して、サーバ装置１００と接続されている。

【００２９】

送受信部２０１は、制御部２０８の制御の基に、インターネット２０を介して、サーバ装置１００から、５個の暗号化コンテンツ鍵ＥＫｃ１、ＥＫｃ２、・・・、ＥＫｃ５、ハッシュ値Ｈ及び暗号化コンテンツＥＣを受け取り、受け取った５個の暗号化コンテンツ鍵ＥＫｃ１、ＥＫｃ２、・・・、ＥＫｃ５を第１復号部２０２へ出力し、受け取ったハッシュ値Ｈを判定部２０４へ出力し、受け取った暗号化コンテンツＥＣを第２復号部２０６へ出力する。

【００３０】

（３）第１復号部２０２

第１復号部２０２は、制御部２０８の制御の基に、送受信部２０１から５個の暗号化コンテンツ鍵ＥＫｃ１、ＥＫｃ２、・・・、ＥＫｃ５を受け取り、情報記憶部２０５から秘密鍵Ｋｓを読み出す。次に、第１復号部２０２は、制御部２０８の制御の基に、以下の処理（ａ）～（ｃ）を５回繰り返す。

【００３１】

（ａ）秘密鍵Ｋｓを用いて、暗号化コンテンツ鍵ＥＫｃｉに対して、復号アルゴリズムＤｅｃ１を施して、コンテンツ鍵ＤＫｃｉを生成する。

ＤＫｃｉ＝Ｄｅｃ１（Ｋｓ、ＥＫｃｉ）

ここで、復号アルゴリズムＤｅｃ１は、ＮＴＲＵ暗号によるアルゴリズムであり、暗号化アルゴリズムＥｎｃ１により生成された暗号文を復号する。Ｚ＝Ｄｅｃ１（Ｙ、Ｘ）は、鍵Ｙを用いて、暗号文Ｘに対して復号アルゴリズムＤｅｃ１を施して復号文Ｚを得ることを示す。

【００３２】

（ｂ）次に、生成したコンテンツ鍵ＤＫｃｉのうち、末尾の６４ビットの乱数部分を削除する。

（ｃ）乱数部分が削除されたコンテンツ鍵ＤＫｃｉをハッシュ部２０３及び判定部２０４へ出力する。

こうして、５個のコンテンツ鍵ＤＫｃｉが、ハッシュ部２０３及び判定部２０４へ出力される。

【００３３】

（４）ハッシュ部２０３

ハッシュ部２０３は、制御部２０８の制御の基に、以下の処理（ａ）～（ｂ）を５回繰り返す。

（ａ）第１復号部２０２からコンテンツ鍵ＤＫｃｉを受け取る。

（ｂ）受け取ったコンテンツ鍵ＤＫｃｉに対して、ハッシュ関数Ｈａｓｈを施して、ハッシュ値Ｈｉを生成する。

【００３４】

Ｈｉ＝Ｈａｓｈ（ＤＫｃｉ）

次に、ハッシュ部２０３は、生成したハッシュ値Ｈｉを判定部２０４へ出力する。

（５）判定部２０４

判定部２０４は、制御部２０８の制御の基に、送受信部２０１からハッシュ値Ｈを受け取り、以下の処理（ａ）～（ｄ）を５回繰り返す。

【００３５】

（ａ）ハッシュ部２０３からハッシュ値Ｈｉを受け取る。

（ｂ）第１復号部２０２からコンテンツ鍵ＤＫｃｉを受け取る。

（ｃ）ハッシュ値Ｈとハッシュ値Ｈｉとが一致しているか否かを判定する。

（ｄ）一致している場合に、ｉの値とコンテンツ鍵ＤＫｃｉとを対応付けて記憶する。

【００３６】

上記の処理（ａ）～（ｂ）の５回の繰り返しが終了した後、記憶しているｉの値があれば、暗号化コンテンツ鍵の復号が正しく行われたものと判断し、ｉの値と対応付けて記憶しているコンテンツ鍵ＤＫｃｉを第２復号部２０６へ出力し、復号が正しく行われたことを示す復号結果を制御部２０８へ出力する。

記憶しているｉの値がなければ、暗号化コンテンツ鍵の復号が正しく行われなかったものと判断し、その旨を示す復号結果を制御部２０８へ出力する。

【００３７】

（６）第２復号部２０６

第２復号部２０６は、制御部２０８の制御の基に、判定部２０４からコンテンツ鍵ＤＫｃｉを受け取り、送受信部２０１から暗号化コンテンツＥＣを受け取り、受け取ったコンテンツ鍵ＤＫｃｉを用いて、受け取った暗号化コンテンツＥＣに復号アルゴリズムＤｅｃ２を施して、コンテンツＣを生成する。

【００３８】

ここで、復号アルゴリズムＤｅｃ２は、トリプルＤＥＳによるアルゴリズムであり、暗号化アルゴリズムＥｎｃ２により生成された暗号文を復号する。

次に、第２復号部２０６は、生成したコンテンツＣを再生部２０７へ出力する。

（７）再生部２０７

再生部２０７は、制御部２０８の制御の基に、第２復号部２０６からコンテンツＣを受け取り、受け取ったコンテンツＣを再生して、映像信号と音声信号とを生成し、生成した映像信号と音声信号とをそれぞれ、モニタ５０及びスピーカ４０へ出力する。

【００３９】

モニタ５０及びスピーカ４０は、それぞれ映像と音声とを出力する。

（８）制御部２０８、入力部２０９及び表示部２１０

制御部２０８は、送受信部２０１、第１復号部２０２、ハッシュ部２０３、判定部２０４、第２復号部２０６及び再生部２０７を制御する。

制御部２０８は、判定部２０４から、暗号化コンテンツ鍵の復号が正しく行われた旨及び正しく行われなかった旨をそれぞれ示す復号結果を受け取る。

【００４０】

正しく行われなかった旨を示す復号結果を受け取ると、第２復号部２０６に対して復号を行わないように制御し、表示部２１０に対して、復号エラーを表示するように制御する。

正しく行われた旨を示す復号結果を受け取ると、第２復号部２０６に対して復号を行うように制御する。

【００４１】

入力部２０９は、映像再生装置２００の利用者から操作指示を受け付け、受け付けた指示を制御部２０８へ出力する。

表示部２１０は、制御部２０８の制御の基に、各種の情報を表示する。

１．３　映像再生システム１０の動作

映像再生システム１０の動作について説明する。

【００４２】

（１）サーバ装置１００の動作

サーバ装置１００の動作について、図４に示すフローチャートを用いて説明する。

第１暗号化部１０３は、情報記憶部１０１からコンテンツ鍵Ｋｃを読み出し

（ステップＳ１０１）、次に、公開鍵Ｋｐを読み出す（ステップＳ１０２）。

【００４３】

次に、制御部１０７は、ステップＳ１０３～Ｓ１０６において、ステップＳ１０４～Ｓ１０５を５回繰り返すように制御する。なお、以下に記載の乱数Ｒｉ及び暗号化コンテンツ鍵ＥＫｃｉの表記における「ｉ」は、繰り返しの各回を示すサフィクスであり、繰り返しにおいて、ｉ＝１、２、３、４、５のように変化するものである。

【００４４】

乱数生成部１０２は、６４ビットの乱数Ｒｉを生成し、生成した乱数Ｒｉを第１暗号化部１０３へ出力し（ステップＳ１０４）、第１暗号化部１０３は、コンテンツ鍵Ｋｃ及び乱数Ｒｉを結合し、公開鍵Ｋｐを用いて、コンテンツ鍵Ｋｃ及び乱数Ｒｉの結合に対して、暗号化アルゴリズムＥｎｃ１を施して、暗号化コンテンツ鍵ＥＫｃｉを生成する（ステップＳ１０５）。

【００４５】

このようにしてステップＳ１０４からステップＳ１０５までが５回繰り返されることにより、５個の暗号化コンテンツ鍵ＥＫｃ１、ＥＫｃ２、・・・、ＥＫｃ５が生成される。

次に、ハッシュ部１０４は、情報記憶部１０１からコンテンツ鍵Ｋｃを読み出し、読み出したコンテンツ鍵Ｋｃに対して、一方向性関数であるハッシュ関数Ｈａｓｈを施して、ハッシュ値Ｈを生成する（ステップＳ１０７）。

【００４６】

次に、第２暗号化部１０５は、情報記憶部１０１からコンテンツ鍵Ｋｃを読み出し（ステップＳ１０８）、コンテンツＣを読み出し（ステップＳ１０９）、読み出したコンテンツ鍵Ｋｃを用いて、読み出したコンテンツＣに暗号化アルゴリズムＥｎｃ２を施して、暗号化コンテンツＥＣを生成する（ステップＳ１１０）。

【００４７】

次に、送受信部１０６は、５個の暗号化コンテンツ鍵ＥＫｃ１、ＥＫｃ２、・・・、ＥＫｃ５、ハッシュ値Ｈ及び暗号化コンテンツＥＣを、インターネット２

０を介して、映像再生装置２００へ送信する（ステップＳ１１１）。

（２）映像再生装置２００の動作

映像再生装置２００の動作について、図５～図６に示すフローチャートを用いて説明する。

【００４８】

送受信部２０１は、インターネット２０を介して、サーバ装置１００から、５個の暗号化コンテンツ鍵ＥＫｃ１、ＥＫｃ２、・・・、ＥＫｃ５、ハッシュ値Ｈ及び暗号化コンテンツＥＣを受け取り、受け取った５個の暗号化コンテンツ鍵ＥＫｃ１、ＥＫｃ２、・・・、ＥＫｃ５を第１復号部２０２へ出力し、受け取ったハッシュ値Ｈを判定部２０４へ出力し、受け取った暗号化コンテンツＥＣを第２復号部２０６へ出力する（ステップＳ１３１）。

【００４９】

第１復号部２０２は、情報記憶部２０５から秘密鍵Ｋｓを読み出す（ステップＳ１３２）。次に、制御部２０８は、ステップＳ１３３～Ｓ１３９において、ステップＳ１３４～Ｓ１３８を５回繰り返すように制御する。なお、以下の暗号化コンテンツ鍵ＥＫｃｉ、コンテンツ鍵ＤＫｃｉ及びハッシュ値Ｈｉの表記における「ｉ」は、繰り返しの各回を示すサフィクスであり、繰り返しにおいて、ｉ＝１、２、３、４、５のように変化するものである。

【００５０】

第１復号部２０２は、秘密鍵Ｋｓを用いて、暗号化コンテンツ鍵ＥＫｃｉに対して、復号アルゴリズムＤｅｃ１を施して、コンテンツ鍵ＤＫｃｉを生成し（ステップＳ１３４）、次に、生成したコンテンツ鍵ＤＫｃｉのうち、末尾の６４ビットの乱数部分を削除し、乱数部分が削除されたコンテンツ鍵ＤＫｃｉをハッシュ部２０３及び判定部２０４へ出力する（ステップＳ１３５）。

【００５１】

次に、ハッシュ部２０３は、第１復号部２０２からコンテンツ鍵ＤＫｃｉを受け取り、受け取ったコンテンツ鍵ＤＫｃｉに対して、ハッシュ関数Ｈａｓｈを施して、ハッシュ値Ｈｉを生成する（ステップＳ１３６）。

次に、判定部２０４は、ハッシュ部２０３からハッシュ値Ｈｉを受け取り、第

１復号部２０２からコンテンツ鍵ＤＫｃｉを受け取り、ハッシュ値Ｈとハッシュ値Ｈｉとが一致しているか否かを判定し（ステップＳ１３７）、一致している場合に（ステップＳ１３７）、このときのｉの値とコンテンツ鍵ＤＫｃｉとを対応付けて記憶する（ステップＳ１３８）。

【００５２】

ステップＳ１３４～Ｓ１３８が５回繰り返し行われた後で、記憶しているｉの値があれば（ステップＳ１４０）、暗号化コンテンツ鍵の復号が正しく行われたものと判断し、第２復号部２０６は、判定部２０４からコンテンツ鍵ＤＫｃｉを受け取り、送受信部２０１から暗号化コンテンツＥＣを受け取り、受け取ったコンテンツ鍵ＤＫｃｉを用いて、受け取った暗号化コンテンツＥＣに復号アルゴリズムＤｅｃ２を施して、コンテンツＣを生成し（ステップＳ１４１）、再生部２０７は、第２復号部２０６からコンテンツＣを受け取り、受け取ったコンテンツＣを再生して、映像信号と音声信号とを生成し、生成した映像信号と音声信号とをそれぞれ、モニタ５０及びスピーカ４０へ出力し、モニタ５０及びスピーカ４０は、それぞれ映像と音声とを出力する（ステップＳ１４２）。

【００５３】

記憶しているｉの値がなければ（ステップＳ１４０）、判定部２０４は、５個の暗号化コンテンツ鍵の復号が全て正しく行われなかったものと判断し、その旨を示す復号結果を制御部２０８へ出力し、制御部２０８は、第２復号部２０６に対して復号を行わないように制御し、表示部２１０に対して、復号エラーを表示するように制御し、表示部２１０は、復号エラーを表示する（ステップＳ１４３）。

【００５４】

なお、上記において、制御部２０８は、ステップＳ１３３～Ｓ１３９において、ステップＳ１３４～Ｓ１３８を５回繰り返すように制御するとしているが、ステップＳ１３７において、ハッシュ値Ｈとハッシュ値Ｈｉとが一致していると判定された場合に、ステップＳ１３４～Ｓ１３８のループを抜けるとしてもよい。

１．４　まとめ

以上説明したように、上記の実施の形態では、メッセージｍ（実施の形態では

、コンテンツ鍵）を複数回暗号化して送信することにより、メッセージmが復元不可能となる確率を小さくするようにしている。こうして、メッセージmの再送要求の発生確率が小さくなる。

【００５５】

送信装置（実施の形態では、サーバ装置）は、乱数Ｒ１～Ｒ５を生成し、ｍ｜｜Ｒ１、ｍ｜｜Ｒ２、ｍ｜｜Ｒ３、ｍ｜｜Ｒ４及びｍ｜｜Ｒ５を生成し、それぞれを暗号化してＥｎｃ（ｍ｜｜Ｒ１）、Ｅｎｃ（ｍ｜｜Ｒ２）、Ｅｎｃ（ｍ｜｜Ｒ３）、Ｅｎｃ（ｍ｜｜Ｒ４）及びＥｎｃ（ｍ｜｜Ｒ５）を生成する。ここで、Ｅｎｃ（Ｘ）は、平文Ｘに暗号化アルゴリズムＥｎｃを施して暗号文を生成することを示している。次に、ハッシュ値Ｈ（ｍ）を計算する。次に、Ｅｎｃ（ｍ｜｜Ｒ１）、Ｅｎｃ（ｍ｜｜Ｒ２）、Ｅｎｃ（ｍ｜｜Ｒ３）、Ｅｎｃ（ｍ｜｜Ｒ４）、Ｅｎｃ（ｍ｜｜Ｒ５）及びハッシュ値Ｈ（ｍ）を受信装置（実施の形態では、映像再生装置）へ送信する。

【００５６】

受信装置は、Ｅｎｃ（ｍ｜｜Ｒ１）、Ｅｎｃ（ｍ｜｜Ｒ２）、Ｅｎｃ（ｍ｜｜Ｒ３）、Ｅｎｃ（ｍ｜｜Ｒ４）、Ｅｎｃ（ｍ｜｜Ｒ５）及びハッシュ値Ｈ（ｍ）を受信し、Ｅｎｃ（ｍ｜｜Ｒ１）、Ｅｎｃ（ｍ｜｜Ｒ２）、Ｅｎｃ（ｍ｜｜Ｒ３）、Ｅｎｃ（ｍ｜｜Ｒ４）、Ｅｎｃ（ｍ｜｜Ｒ５）を復号して、メッセージに相当する部分ｍ１、・・・、ｍ５を取得する。さらに、ｍ１、・・・、ｍ５のハッシュ値Ｈ（ｍ１）、・・・、Ｈ（ｍ５）を計算し、それぞれ計算したハッシュ値と受信したハッシュ値Ｈ（ｍ）とを比較する。この比較において、計算したハッシュ値と受信したハッシュ値Ｈ（ｍ）とが一致するものが、１組でも存在するならば、一致するハッシュ値に対応するメッセージ（ｍ１、・・・、ｍ５のいずれか）を復号文として出力する。ハッシュ値が一致するものが全く存在しなければ、復号エラーを示すＦａｌｓｅを出力する。

【００５７】

２６３次元のＮＴＲＵ暗号において、暗号文の１つ１つが復号エラーを起こす確率は、１０-5程度である。上記の実施の形態では、５個の暗号文を送信するので、再生要求が発生する確率は、１０-25（＝１０-5×１０-5×１０-5×１０-5

×１０$^{-5}$）程度となる。一方、１０２４ビットのＲＳＡ暗号の場合における攻撃成功確率は、２$^{-80}$＝１０$^{-24}$である。このため、２６３次元のＮＴＲＵ暗号において、上記の実施の形態を適用した場合には、１０２４ビットのＲＳＡ暗号の場合における攻撃成功確率を下回ることとなる。

【００５８】

２．その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

（１）上記の実施の形態では、コンテンツ鍵を暗号化して生成した暗号化コンテンツ鍵を５個送信するとしているが、コンテンツを暗号化して生成した暗号化コンテンツを５個送信するとしてもよい。

【００５９】

（２）上記の実施の形態では、送信装置は、５個の暗号文を生成して送信し、受信装置は、５個の暗号文を受信して復号するとしているが、暗号文の生成個数が５個に限定されることはない。例えば、３個でもよいし、７個でもよい。送信装置は、２個以上の暗号文を生成して送信し、受信装置は、これらの暗号文を受信して復号し、これらの結果により、復号時のエラーの判定を行うとしてもよい。上述したように、暗号文の個数は、攻撃成功確率に影響し、暗号文の個数が多ければ多いほど、攻撃成功確率は、低くなる。

【００６０】

（３）上記の実施の形態では、暗号化されるメッセージｍとその都度生成した乱数との結合体に対して暗号化アルゴリズムを施すとしているが、送信装置は、メッセージｍに対してさらに他の演算を施して、演算結果と乱数との結合体に対して暗号化アルゴリズムを施すとしてもよい。

例えば、送信装置は、メッセージｍに、「０」、「１」、「２」、「３」及び「４」をそれぞれ加算して「ｍ」、「ｍ＋１」、「ｍ＋２」、「ｍ＋３」及び「ｍ＋４」を算出し、それぞれの算出結果と乱数との結合体に対して暗号化アルゴリズムを施して、

Ｅｎｃ（ｍ｜｜Ｒ１）、Ｅｎｃ（ｍ＋１｜｜Ｒ２）、Ｅｎｃ（ｍ＋２｜｜Ｒ３）、Ｅｎｃ（ｍ＋３｜｜Ｒ４）、Ｅｎｃ（ｍ＋４｜｜Ｒ５）を生成する。

【００６１】

受信装置は、Ｅｎｃ（ｍ｜｜Ｒ１）、Ｅｎｃ（ｍ＋１｜｜Ｒ２）、Ｅｎｃ（ｍ＋２｜｜Ｒ３）、Ｅｎｃ（ｍ＋３｜｜Ｒ４）、Ｅｎｃ（ｍ＋４｜｜Ｒ５）を復号し、それぞれの復号結果から、末尾の所定長の乱数部分を削除し、乱数部分が削除された復号結果から、「０」、「１」、「２」、「３」及び「４」をそれぞれ減じてメッセージｍに相当する情報を得る。

【００６２】

（４）上記の実施の形態では、送信装置は、メッセージｍと乱数とをこの順序で結合し、結合結果に対して暗号化アルゴリズムを施すとしているが、結合の順序を逆にしてもよい。つまり、乱数とメッセージｍとをこの順序で結合するとしていもよい。また、メッセージｍと乱数とを１ビットずつ交互に結合してもよい。このとき、受信装置は、それぞれ逆の演算を行うことにより、メッセージｍに相当する情報を得ることができる。

【００６３】

（５）上記の実施の形態では、サーバ装置は、インターネットを介して、５個の暗号化コンテンツ鍵、暗号化コンテンツ及びハッシュ値を、映像再生装置へ送信するとしているが、この実施の形態に限定されることはない。

サーバ装置に代えてデジタル放送送信装置により、５個の暗号化コンテンツ鍵、暗号化コンテンツ及びハッシュ値を、インターネットに代えてデジタル放送波に載せて放送し、映像再生装置に代えてデジタル放送受信装置は、デジタル放送波を受信し、受信したデジタル放送波から５個の暗号化コンテンツ鍵、暗号化コンテンツ及びハッシュ値を抽出するとしてもよい。

【００６４】

（６）映像再生システム１０は、映像再生装置２００に代えて、図７に示す映像再生装置２００ｂ及びメモリカード３００ｂを含むとしてもよい。

映像再生装置２００ｂは、映像再生装置２００の一部の機能を備え、メモリカード３００ｂは、映像再生装置２００の他の一部の機能を備える。

つまり、メモリカード３００ｂは、利用者により映像再生装置２００ｂに装着され、映像再生装置２００ｂを介して、サーバ装置１００から、５個の暗号化コンテンツ鍵とハッシュ値とを受け取り、各暗号化コンテンツ鍵が正しく復号されるか否かを判定し、正しく復号されると判定する場合に、正しく復号されたコンテンツ鍵を映像再生装置２００ｂへ出力する。映像再生装置２００ｂは、メモリカード３００ｂからコンテンツ鍵を受け取り、サーバ装置１００から受け取った暗号化コンテンツを復号して再生する。

【００６５】

具体的には、映像再生装置２００ｂは、図７に示すように、送受信部２０１、第２復号部２０６、再生部２０７、制御部２０８、入力部２０９、表示部２１０、入出力部２１１及び認証部２１２から構成されている。

ここで、映像再生装置２００ｂの構成要素である送受信部２０１、第２復号部２０６、再生部２０７、制御部２０８、入力部２０９及び表示部２１０は、それぞれ、映像再生装置２００の構成要素である送受信部２０１、第２復号部２０６、再生部２０７、制御部２０８、入力部２０９及び表示部２１０と同様のものである。また、入出力部２１１は、メモリカード３００ｂと映像再生装置２００ｂの他の構成要素との間で情報の入出力を行う。さらに、認証部２１２は、何らかのメモリカードが映像再生装置２００ｂに装着されたときに、装着されたメモリカードとの間で、相互の機器認証を行う。機器認証が成功した場合に限り、その後の入出力が行われる。

【００６６】

また、メモリカード３００ｂは、図７に示すように、入出力部３０１、認証部３０２、第１復号部２０２ｂ、ハッシュ部２０３ｂ、判定部２０４ｂ、情報記憶部２０５ｂから構成されている。

ここで、第１復号部２０２ｂ、ハッシュ部２０３ｂ、判定部２０４ｂ及び情報記憶部２０５ｂは、それぞれ、映像再生装置２００の構成要素である第１復号部２０２、ハッシュ部２０３、判定部２０４及び情報記憶部２０５と同様のものである。また、入出力部３０１は、メモリカード３００ｂの他の構成要素と映像再生装置２００ｂとの間で情報の入出力を行う。さらに、認証部３０２は、メモリ

カード３００ｂが何らかの装置に装着されたときに、装着された装置との間で、相互の機器認証を行う。機器認証が成功した場合に限り、その後の入出力が行われる。

【００６７】

（７）別の実施の形態

本発明に係る別の実施の形態としてのＢＤ再生システム１０ｃについて説明する。

ＢＤ再生システム１０ｃは、図８に示すように、サーバ装置１００ｃ、ＢＤプレイヤ２００ｃ及び携帯電話４００ｃから構成されており、サーバ装置１００ｃと携帯電話４００ｃとは、インターネット２０、携帯電話網２５及び無線基地局２６を介して、接続されている。

【００６８】

（ＢＤ再生システム１０ｃの構成）

サーバ装置１００ｃは、サーバ装置１００と同様の構成を有している。

ＢＤプレイヤ２００ｃは、図９に示すように、ドライブ部２１３、第２復号部２０６、再生部２０７、制御部２０８、入力部２０９、表示部２１０、入出力部２１１及び認証部２１２から構成されている。

【００６９】

ここで、ＢＤプレイヤ２００ｃの構成要素である第２復号部２０６、再生部２０７、制御部２０８、入力部２０９及び表示部２１０は、それぞれ、映像再生装置２００の構成要素である第２復号部２０６、再生部２０７、制御部２０８、入力部２０９及び表示部２１０と同様のものである。また、入出力部２１１は、メモリカード３００ｃとＢＤプレイヤ２００ｃの他の構成要素との間で情報の入出力を行う。さらに、認証部２１２は、何らかのメモリカードがＢＤプレイヤ２００ｃに装着されたときに、装着されたメモリカードとの間で、相互の機器認証を行う。機器認証が成功した場合に限り、その後の入出力が行われる。ドライブ部２１３は、装着されたＢＤ６０から暗号化コンテンツを読み出し、読み出した暗号化コンテンツを第２復号部２０６へ出力する。

【００７０】

また、メモリカード３００ｃは、図９に示すように、入出力部３０１ｃ、認証部３０２ｃ、第１復号部２０２ｃ、ハッシュ部２０３ｃ、判定部２０４ｃ、情報記憶部２０５ｃから構成されている。

ここで、第１復号部２０２ｃ、ハッシュ部２０３ｃ、判定部２０４ｃ及び情報記憶部２０５ｃは、それぞれ、映像再生装置２００の構成要素である第１復号部２０２、ハッシュ部２０３、判定部２０４及び情報記憶部２０５と同様のものである。また、入出力部３０１ｃは、メモリカード３００ｃの他の構成要素とＢＤプレイヤ２００ｃとの間で情報の入出力を行う。さらに、認証部３０２ｃは、メモリカード３００ｃが何らかの装置に装着されたときに、装着された装置との間で、相互の機器認証を行う。機器認証が成功した場合に限り、その後の入出力が行われる。情報記憶部２０５は、秘密鍵Ｋｓ、５個の暗号化コンテンツ鍵、ハッシュ値及び再生されたコンテンツ鍵を記憶するための領域を備えている。

【００７１】

（ＢＤ再生システム１０ｃの動作）

コンテンツ鍵を用いてコンテンツを暗号化して生成された暗号化コンテンツを記録しているＢＤ６０が配布され、利用者は、配布されたＢＤ６０を入手する。

コンテンツ鍵は、次に示すように、ＢＤ６０の配布とは異なる別のルートを介して配布される。

【００７２】

サーバ装置１００ｃは、サーバ装置１００と同様に、コンテンツ鍵から５個の暗号化コンテンツ鍵とハッシュ値とを生成し、生成した５個の暗号化コンテンツ鍵とハッシュ値とを、インターネット２０、携帯電話網２５及び無線基地局２６を介して、携帯電話４００ｃへ送信する。

携帯電話４００ｃには、利用者によりメモリカード３００ｃが装着される。

【００７３】

携帯電話４００ｃは、サーバ装置１００ｃから５個の暗号化コンテンツ鍵とハッシュ値とを受信し、受信した５個の暗号化コンテンツ鍵とハッシュ値とをメモリカード３００ｃの入出力部３０１ｃを介して、情報記憶部２０５ｃへ書き込む。

メモリカード３００ｃの情報記憶部２０５ｃは、５個の暗号化コンテンツ鍵とハッシュ値とを一旦記憶し、第１復号部２０２ｃは、情報記憶部２０５ｃから各暗号化コンテンツ鍵を読み出して復号し、復号結果のコンテンツ鍵をハッシュ部２０３ｃ及び判定部２０４ｃへ出力する。判定部２０４ｃは、情報記憶部２０５ｃからハッシュ値を読み出し、読み出したハッシュ値と、第１復号部２０２ｃから受け取った復号結果のコンテンツ鍵とを用いて、各暗号化コンテンツ鍵が正しく復号されるか否かを判定し、正しく復号されると判定する場合に、正しく復号されたコンテンツ鍵を情報記憶部２０５ｃに書き込む。

【００７４】

メモリカード３００ｃ及びＢＤ６０は、利用者により、ＢＤプレイヤ２００ｃに装着される。

ＢＤプレイヤ２００ｃは、ＢＤ６０から暗号化コンテンツを読み出し、メモリカード３００ｃの情報記憶部２０５ｃから正しく復号されたコンテンツ鍵を読み出し、読み出したコンテンツ鍵を用いて、読み出した暗号化コンテンツを復号してコンテンツを生成し、生成したコンテンツを再生し、ＢＤプレイヤ２００ｃに接続されているモニタ５０及びスピーカ４０へ映像及び音声を出力する。

【００７５】

（８）上記の実施の形態において、２６３次元のＮＴＲＵ暗号方式を用いるとし、秘密鍵及び公開鍵のビット長は、それぞれ、４１５ビット、１８４１ビットであるとしているが、これらの次元やビット数には限定されない。

また、ハッシュ部１０４及びハッシュ部２０３は、ハッシュ関数Ｈａｓｈとして、ＳＨＡ－１を用いるとしているが、他のハッシュ関数を用いるとしてもよい。

【００７６】

（９）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディス

ク、ＣＤ―ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【００７７】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【００７８】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（１０）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【００７９】

【発明の効果】

以上説明したように、本発明は、メッセージを秘密に通信する暗号通信システムであって、１個のメッセージを記憶している記憶手段と、前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成する暗号手段と、前記メッセージに一方向性演算を施して比較演算値を生成する演算手段と、生成した前記複数の暗号文と前記比較演算値とを送信する送信手段とを備える暗号送信装置と、前記複数の暗号文と前記比較演算値とを受信する受信手段と、前記複数の暗号文の各々に対して、前記暗号化演算に対応する復号演算により同数の復号メッセージを生成する復号手段と、前記複数の復号メッセージの各々に、前記一方

向性演算を施して、同数の復号演算値を生成する演算手段と、生成した各復号演算値と受信した前記比較演算値とを比較して、少なくとも１組の前記復号演算値と前記比較演算値とが一致すれば、前記メッセージの正当な復号文として、当該組に対応する復号メッセージを出力し、全ての組の前記復号演算値と前記比較演算値とが不一致であれば、復号エラーを出力する判定手段とを備える暗号受信装置とから構成される。また、メッセージを秘密に送信する暗号送信装置であって、１個のメッセージを記憶している記憶手段と、前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成する暗号手段と、前記メッセージに一方向性演算を施して比較演算値を生成する演算手段と、生成した前記複数の暗号文と前記比較演算値とを送信する送信手段とを備える。また、暗号送信装置からメッセージを秘密に受信する暗号受信装置であって、前記暗号送信装置は、１個のメッセージを記憶しており、前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成し、前記メッセージに一方向性演算を施して比較演算値を生成し、生成した前記複数の暗号文と前記比較演算値とを送信し、前記暗号受信装置は、前記複数の暗号文と前記比較演算値とを受信する受信手段と、前記複数の暗号文の各々に対して、前記暗号化演算に対応する復号演算により同数の復号メッセージを生成する復号手段と、前記複数の復号メッセージの各々に、前記一方向性演算を施して、同数の復号演算値を生成する演算手段と、生成した各復号演算値と受信した前記比較演算値とを比較して、少なくとも１組の前記復号演算値と前記比較演算値とが一致すれば、前記メッセージの正当な復号文として、当該組に対応する復号メッセージを出力し、全ての組の前記復号演算値と前記比較演算値とが不一致であれば、復号エラーを出力する判定手段とを備える。

【００８０】

これらの構成によると、暗号送信装置は、メッセージから複数個の暗号文を生成し、前記メッセージに一方向性演算を施して比較演算値を生成し、暗号受信装置は、前記複数の暗号文を復号して同数の復号メッセージを生成し、前記複数の復号メッセージに、前記一方向性演算を施して、同数の復号演算値を生成し、少なくとも１組の前記復号演算値と前記比較演算値とが一致すれば、当該組に対応

する正当な復号メッセージを出力し、全ての組の前記復号演算値と前記比較演算値とが不一致であれば、復号エラーを出力するので、復号時にエラーが発生する確率を低く抑え、再送要求による攻撃を回避できる可能性を高くすることができる。

【００８１】

ここで、前記暗号手段は、前記メッセージに対して、可逆のデータ変換を施して、変換メッセージを生成し、生成した変換メッセージに対して、暗号アルゴリズムを施して暗号文を生成する前記暗号化演算を行う暗号化演算部と、前記暗号化演算部に対して、変換メッセージの生成と暗号文の生成とを前記複数回繰り返すように制御する繰返制御部とを含む。また、前記暗号送信装置は、前記メッセージに対して、可逆のデータ変換を施して、変換メッセージを生成し、生成した変換メッセージに対して、暗号アルゴリズムを施して暗号文を生成する前記暗号化演算を行い、変換メッセージの生成と暗号文の生成とを前記複数回繰り返し、前記復号手段は、前記暗号文に対して、前記暗号アルゴリズムに対応する復号アルゴリズムを施して復号文を生成し、生成した復号文に対して、前記データ変換の逆変換を施して、復号メッセージを生成する前記復号演算を行う復号演算部と、前記復号演算部とに対して、復号文の生成と復号メッセージの生成とを、前記複数回繰り返すように制御する繰返制御部とを含む。

【００８２】

これらの構成によると、暗号送信装置は、メッセージに対して、可逆のデータ変換を施して生成した変換メッセージに対して、暗号アルゴリズムを施して暗号文を生成するので、送信される暗号文が送信路で盗聴され、解読された場合であっても、元のメッセージの復号が容易に知られないようにすることができる。また、暗号受信装置は、前記暗号文に対して、前記暗号アルゴリズムに対応する復号アルゴリズムを施して生成した復号文に対して、前記データ変換の逆変換を施して、復号メッセージを生成するので、メッセージに相当する復号メッセージを確実に得ることができる。

【００８３】

ここで、前記暗号化演算部は、固定長の乱数を生成し、前記メッセージに対し

て、生成した前記乱数を付加することにより、前記変換メッセージを生成する。また、前記暗号送信装置は、固定長の乱数を生成し、前記メッセージに対して、生成した前記乱数を付加することにより、前記変換メッセージを生成し、前記復号演算部は、生成した復号文から、前記固定長の乱数部分を除去して復号メッセージを生成する。

【００８４】

これらの構成によると、暗号送信装置は、前記メッセージに対して、固定長の乱数を付加して変換メッセージを生成するので、逆変換が容易である。また、暗号受信装置は、生成した復号文から、前記固定長の乱数部分を除去して復号メッセージを生成するので、メッセージに相当する復号メッセージを確実に得ることができる。

【図面の簡単な説明】

【図１】

本発明に係る１個の実施の形態としての映像再生システム１０の構成を示すシステム構成図である。

【図２】

サーバ装置１００の構成を示す機能ブロック図である。

【図３】

映像再生装置２００の構成を示す機能ブロック図である。

【図４】

サーバ装置１００の動作を示すフローチャートである。

【図５】

映像再生装置２００の動作を示すフローチャートである。図６へ続く。

【図６】

映像再生装置２００の動作を示すフローチャートである。図５から続く。

【図７】

変形例としての映像再生システム１０に含まれる映像再生装置２００ｂ及びメモリカード３００ｂの構成を示す機能ブロック図である。

【図８】

本発明に係る別の実施の形態としてのＢＤ再生システム１０ｃの構成を示すシステム構成図である。

【図９】

ＢＤ再生システム１０ｃに含まれるメモリカード３００ｃ及びＢＤプレイヤ２００ｃの構成を示す機能ブロック図である。

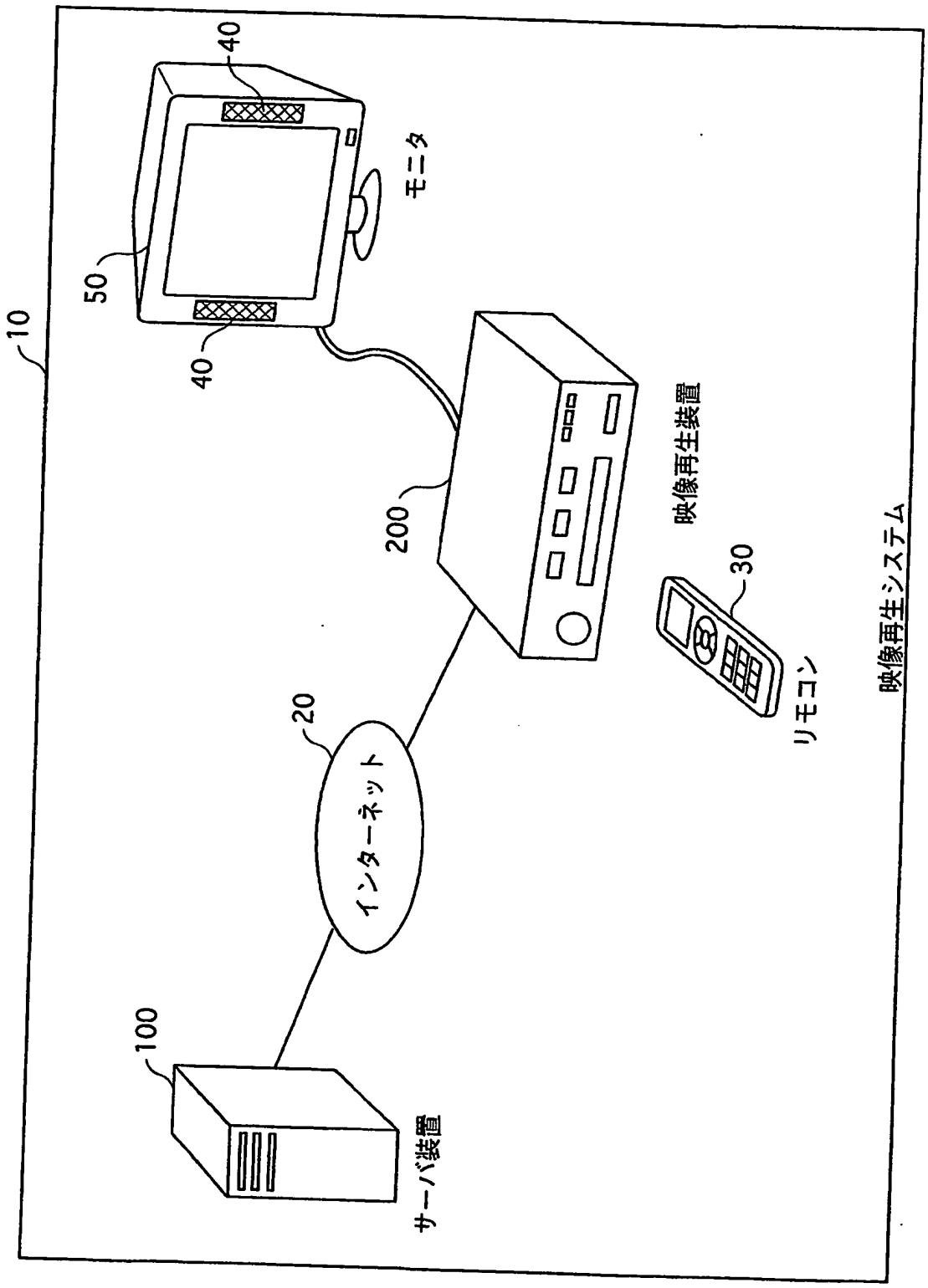
【符号の説明】

１０　映像再生システム
１０ｃ　ＢＤ再生システム
２０　インターネット
２５　携帯電話網
２６　無線基地局
４０　スピーカ
５０　モニタ
６０　ＢＤ
１００、１００ｃ　サーバ装置
１０１　情報記憶部
１０２　乱数生成部
１０３　第１暗号化部
１０４　ハッシュ部
１０５　第２暗号化部
１０６　送受信部
１０７　制御部
１０８　入力部
１０９　表示部
２００、２００ｂ　映像再生装置
２００ｃ　ＢＤプレイヤ
２０１　送受信部
２０２、２０２ｂ、２０２ｃ　第１復号部
２０３、２０３ｂ、２０３ｃ　ハッシュ部

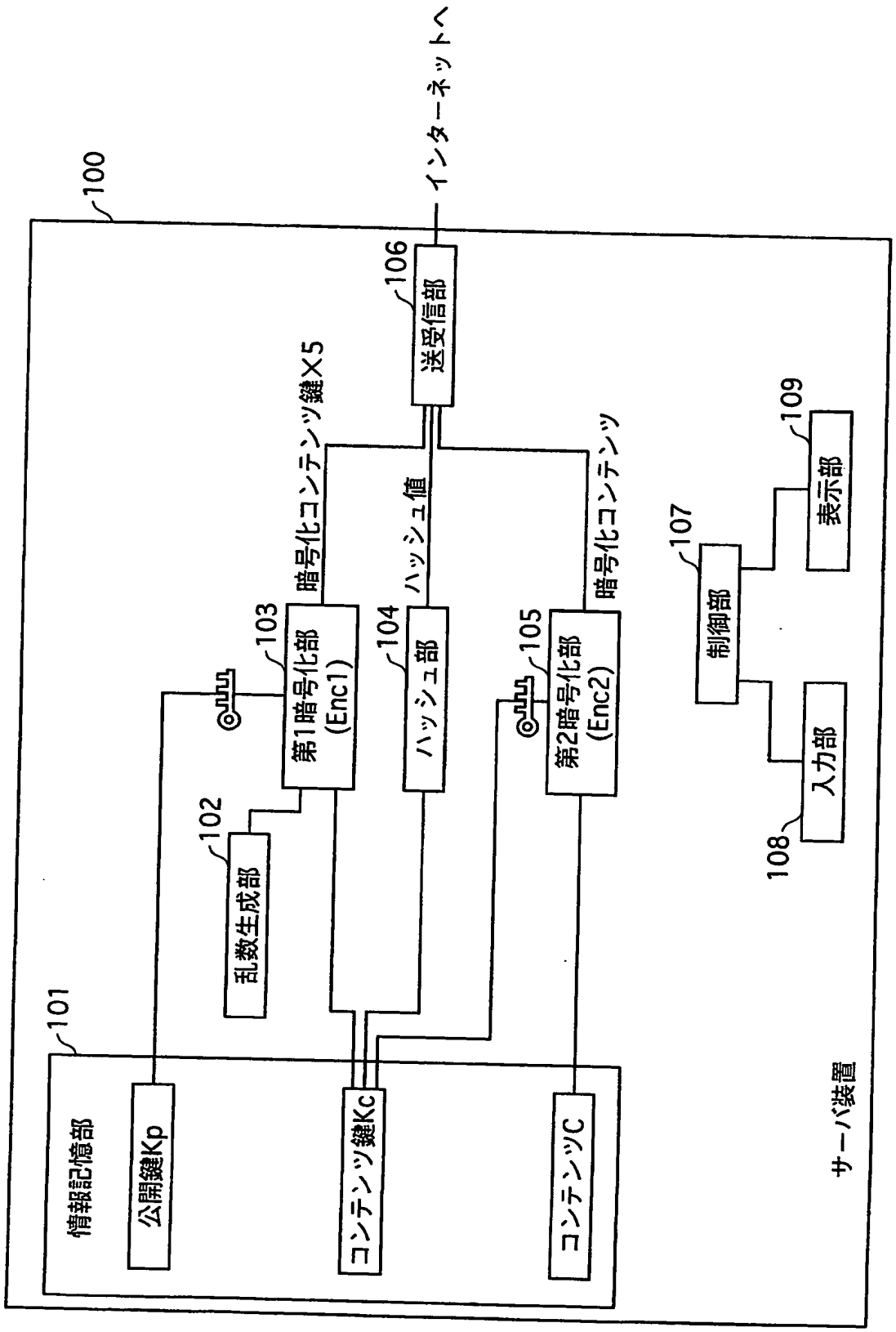
２０４、２０４ｂ、２０４ｃ　判定部
２０５、２０５ｂ、２０５ｃ　情報記憶部
２０６　第２復号部
２０７　再生部
２０８　制御部
２０９　入力部
２１０　表示部
２１１　入出力部
２１２　認証部
２１３　ドライブ部
３００ｂ、３００ｃ　メモリカード
３０１、３０１ｃ　入出力部
３０２、３０２ｃ　認証部
４００ｃ　携帯電話

【書類名】　図面

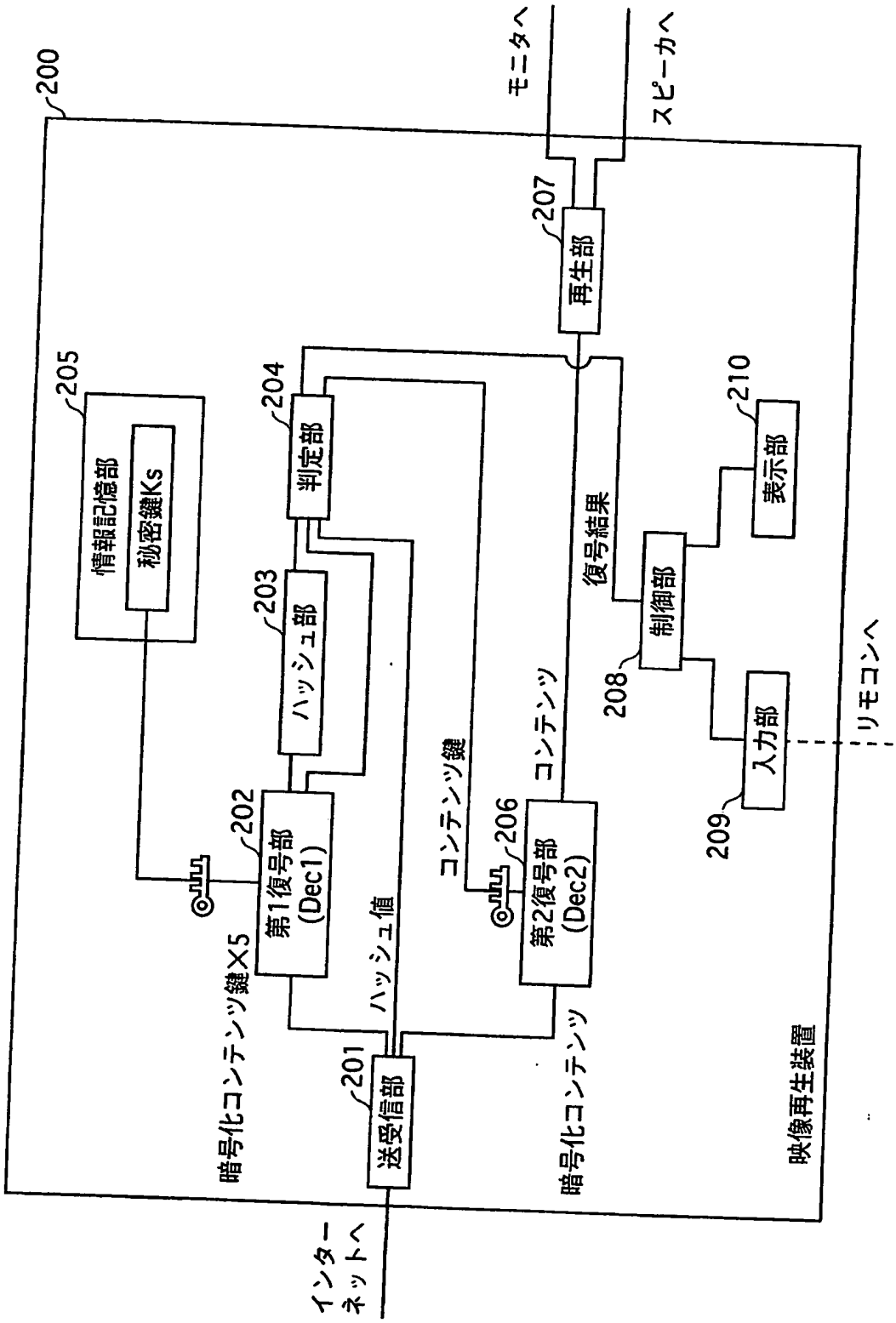
【図１】


10
40
モニタ
50
40
200
映像再生装置
30
リモコン
20
インターネット
100
サーバ装置
映像再生システム

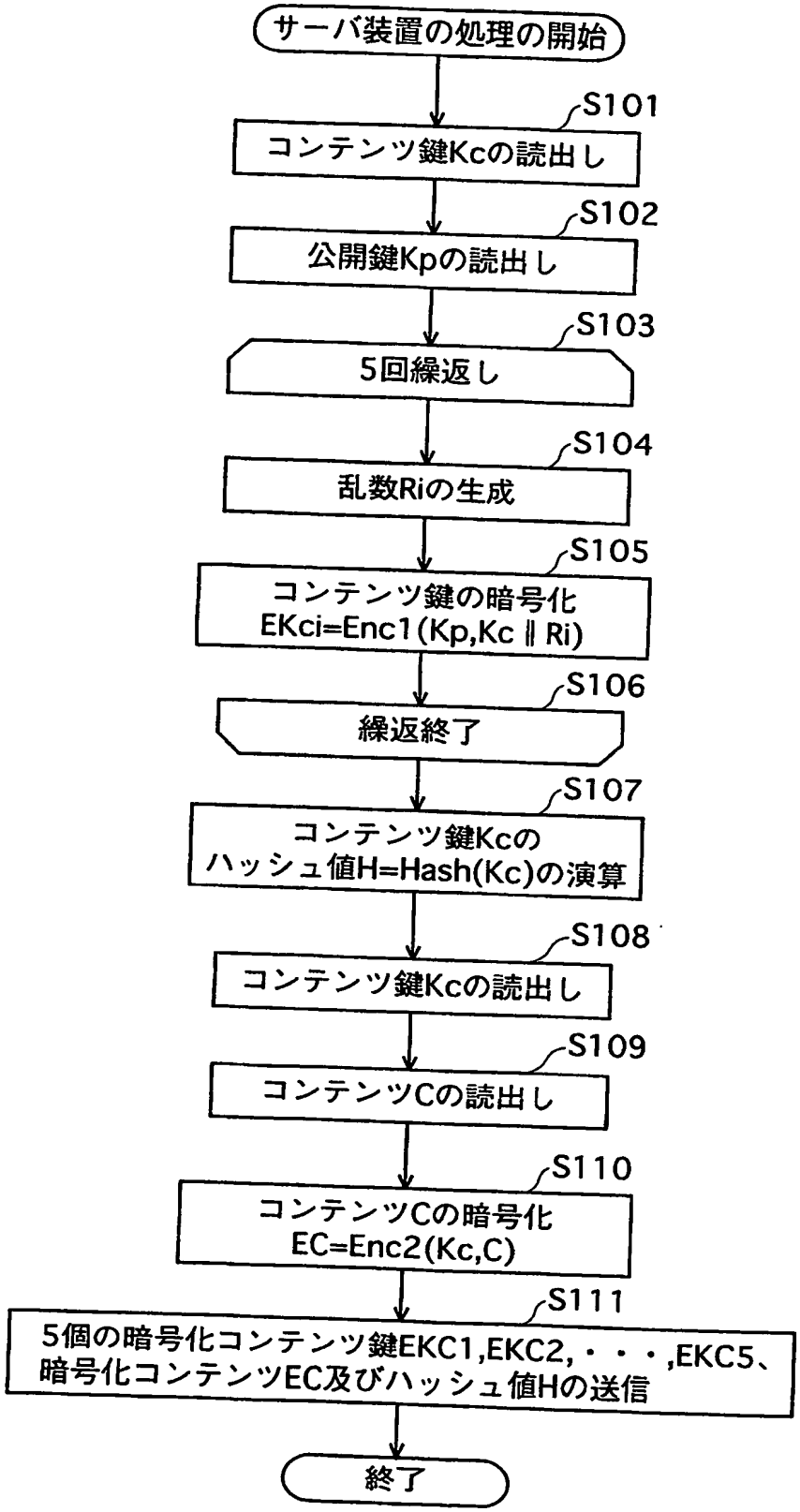
【図２】


100
インターネットへ
106
送受信部
暗号化コンテンツ鍵×5
ハッシュ値
暗号化コンテンツ
109
表示部
107
制御部
103
第1暗号化部
(Enc1)
104
ハッシュ部
105
第2暗号化部
(Enc2)
102
乱数生成部
108
入力部
101
情報記憶部
公開鍵Kp
コンテンツ鍵Kc
コンテンツC
サーバ装置

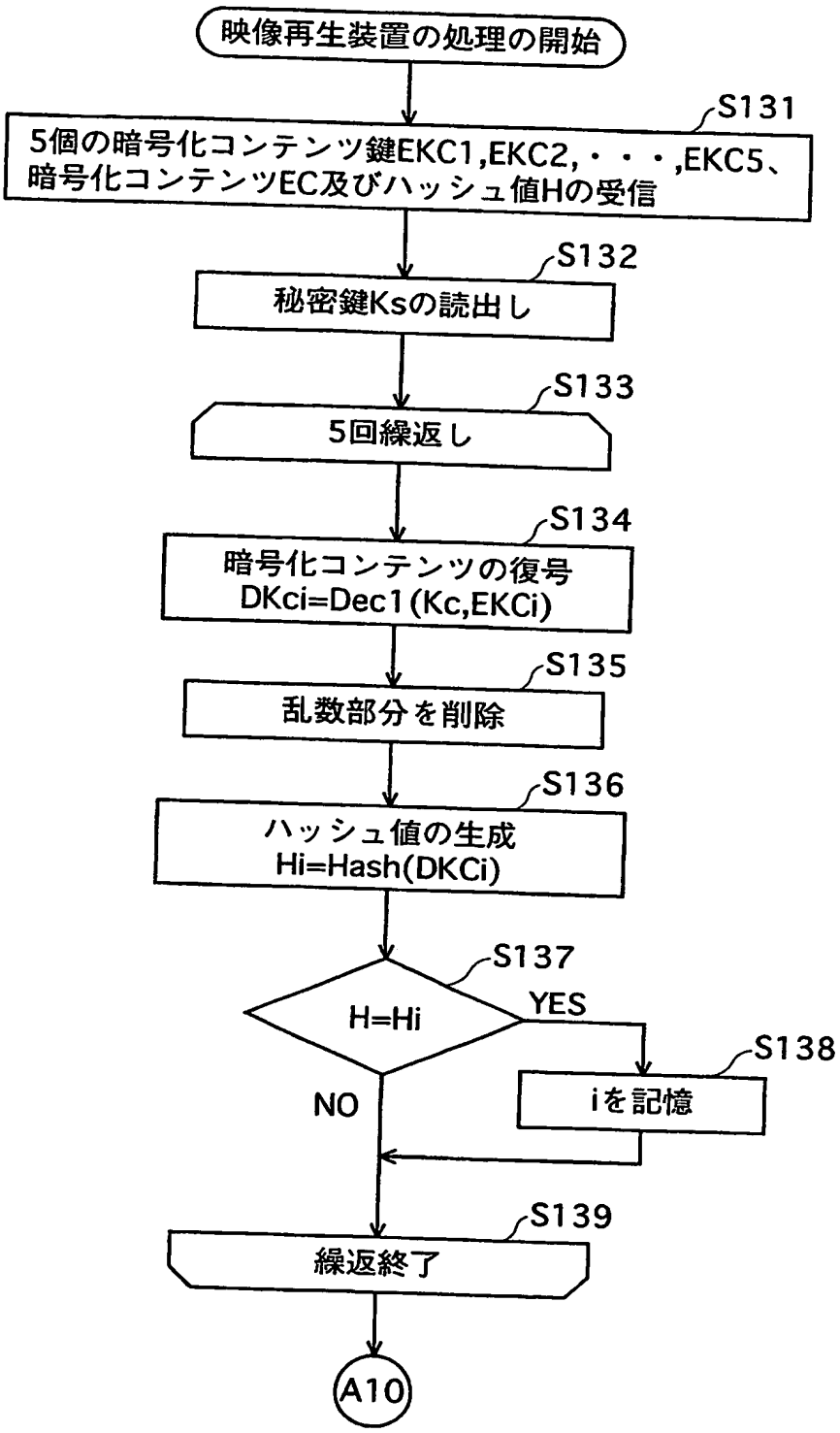
【図３】


200
モニタへ
スピーカへ
207
再生部
205
情報記憶部
秘密鍵Ks
204
判定部
203
ハッシュ部
210
表示部
復号結果
制御部
208
入力部
209
リモコンへ
202
第1復号部
(Dec1)
206
第2復号部
(Dec2)
コンテンツ鍵
コンテンツ
暗号化コンテンツ鍵X5
ハッシュ値
201
送受信部
暗号化コンテンツ
映像再生装置
インター
ネットへ

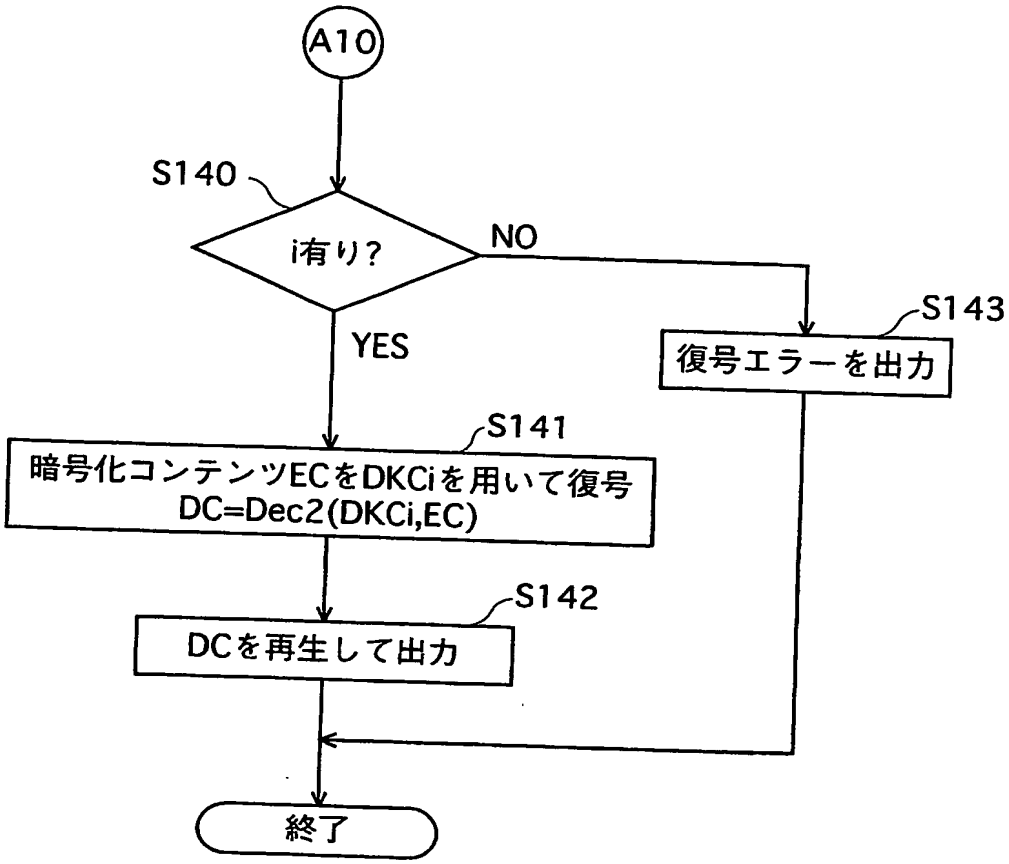
【図４】


サーバ装置の処理の開始
S101
コンテンツ鍵Kcの読出し
S102
公開鍵Kpの読出し
S103
5回繰返し
S104
乱数Riの生成
S105
コンテンツ鍵の暗号化
EKci=Enc1(Kp,Kc‖Ri)
S106
繰返終了
S107
コンテンツ鍵Kcの
ハッシュ値H=Hash(Kc)の演算
S108
コンテンツ鍵Kcの読出し
S109
コンテンツCの読出し
S110
コンテンツCの暗号化
EC=Enc2(Kc,C)
S111
5個の暗号化コンテンツ鍵EKC1,EKC2,・・・,EKC5、
暗号化コンテンツEC及びハッシュ値Hの送信
終了

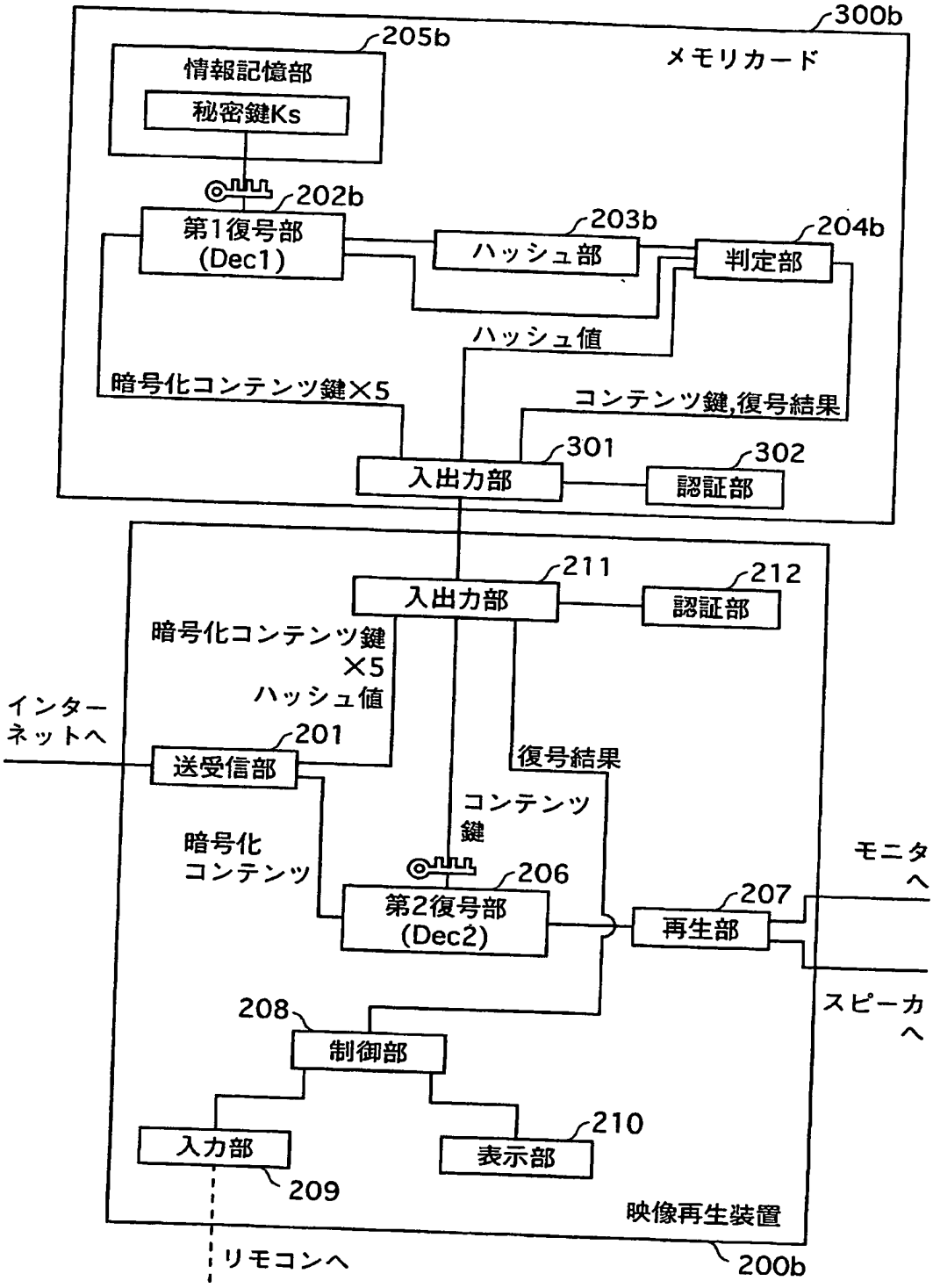
【図５】


映像再生装置の処理の開始
S131
5個の暗号化コンテンツ鍵EKC1,EKC2,・・・,EKC5、
暗号化コンテンツEC及びハッシュ値Hの受信
S132
秘密鍵Ksの読出し
S133
5回繰返し
S134
暗号化コンテンツの復号
DKci=Dec1(Kc,EKCi)
S135
乱数部分を削除
S136
ハッシュ値の生成
Hi=Hash(DKCi)
S137
H=Hi
YES
S138
iを記憶
NO
S139
繰返終了
A10

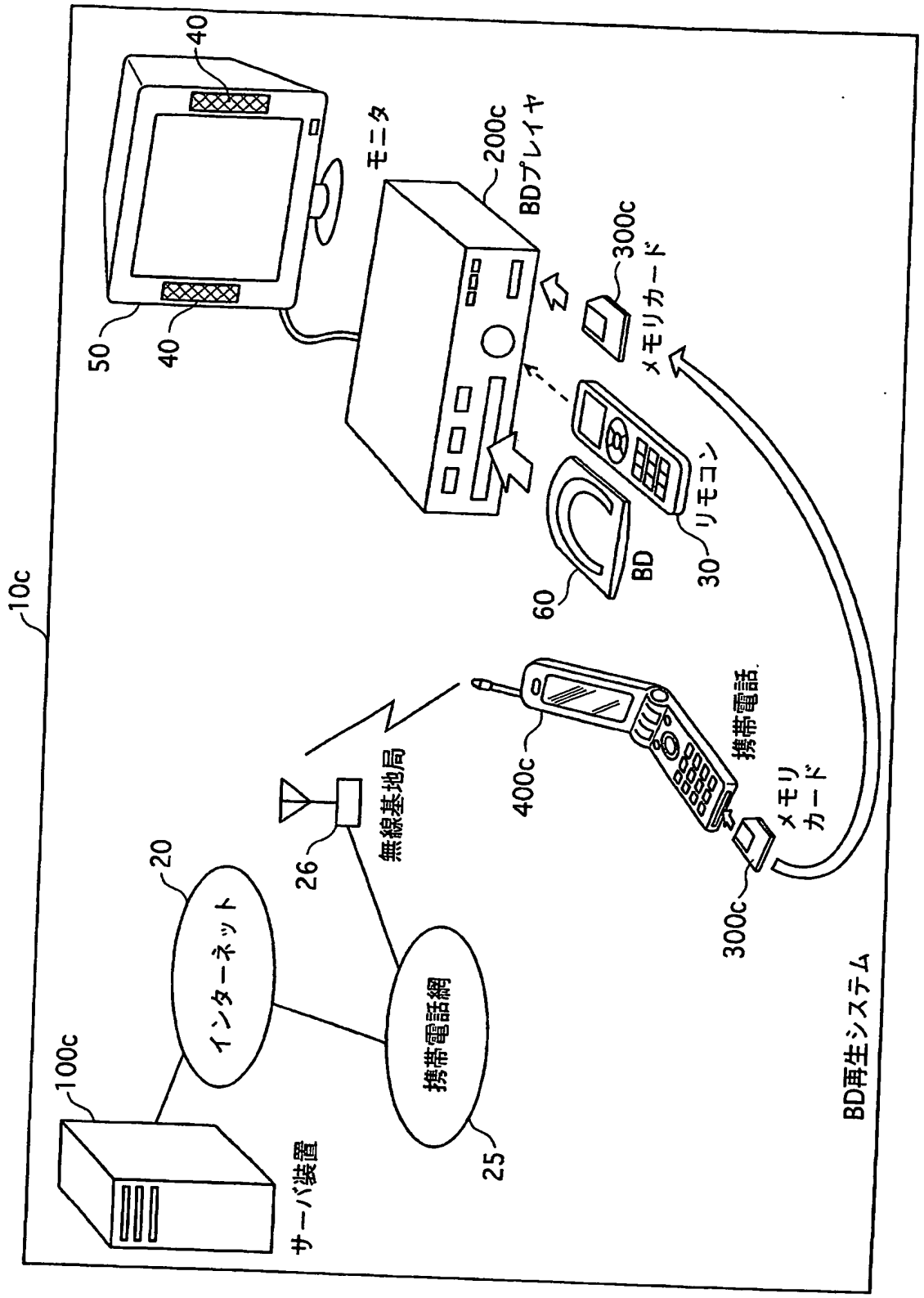
【図６】


A10
S140
i有り?
NO
YES
S143
復号エラーを出力
S141
暗号化コンテンツECをDKCiを用いて復号
DC=Dec2(DKCi,EC)
S142
DCを再生して出力
終了

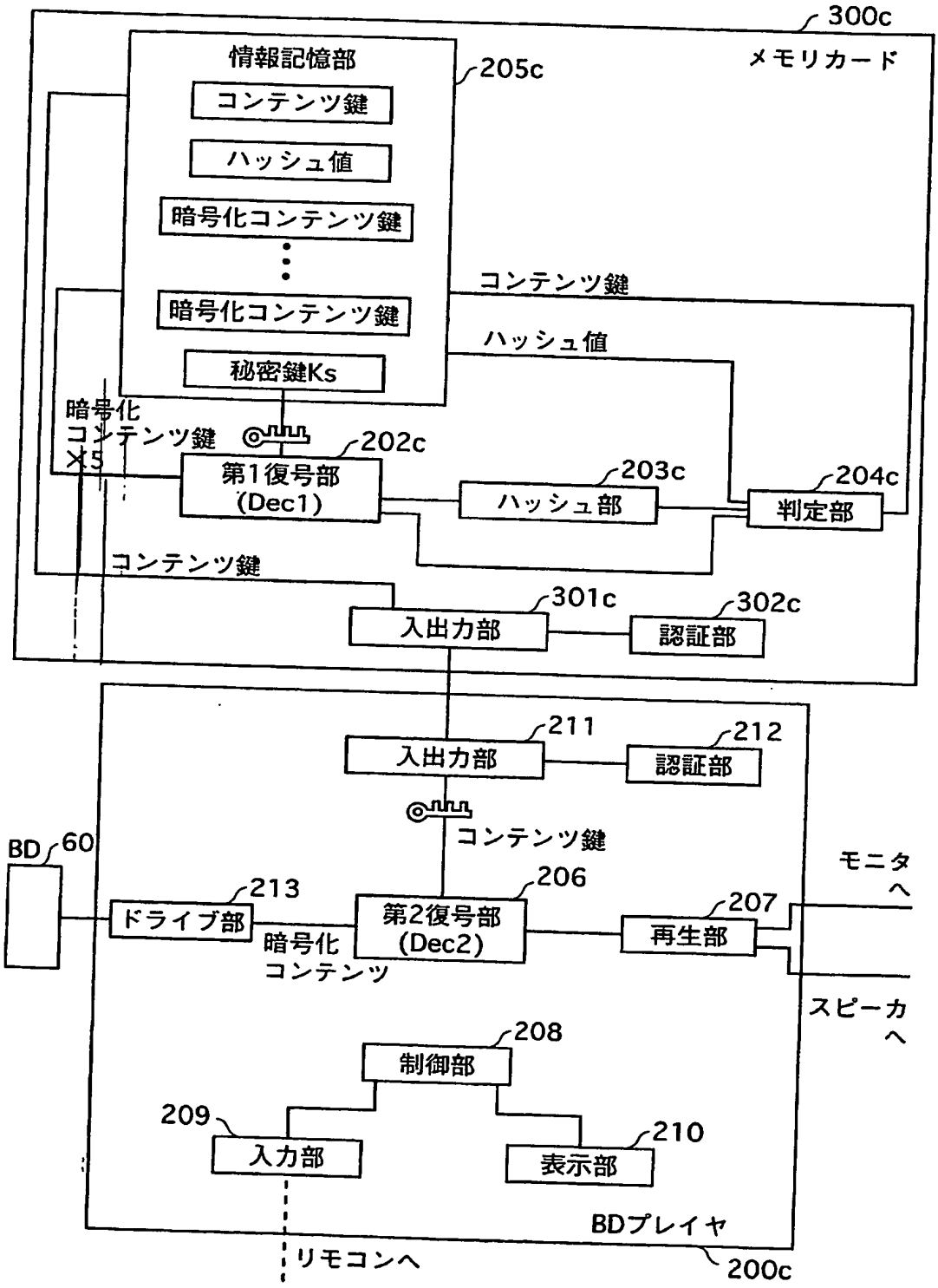
【図７】


300b
メモリカード
205b
情報記憶部
秘密鍵Ks
202b
第1復号部
(Dec1)
203b
ハッシュ部
204b
判定部
ハッシュ値
暗号化コンテンツ鍵×5
コンテンツ鍵,復号結果
301
入出力部
302
認証部
211
入出力部
212
認証部
暗号化コンテンツ鍵
×5
ハッシュ値
インター
ネットへ
201
送受信部
復号結果
コンテンツ
鍵
暗号化
コンテンツ
206
第2復号部
(Dec2)
207
再生部
モニタ
へ
スピーカ
へ
208
制御部
210
表示部
入力部
209
リモコンへ
映像再生装置
200b

【図８】


10c
40
モニタ
200c
BDプレイヤ
300c
メモリカード
50
40
BD
60
リモコン
30
携帯電話
400c
メモリ
カード
300c
無線基地局
26
20
インターネット
携帯電話網
25
100c
サーバ装置
BD再生システム

【図９】


300c
メモリカード
情報記憶部
205c
コンテンツ鍵
ハッシュ値
暗号化コンテンツ鍵
暗号化コンテンツ鍵
秘密鍵Ks
コンテンツ鍵
ハッシュ値
暗号化コンテンツ鍵 Ks
202c
第1復号部 (Dec1)
203c
ハッシュ部
204c
判定部
コンテンツ鍵
301c
入出力部
302c
認証部
211
入出力部
212
認証部
コンテンツ鍵
BD
60
213
ドライブ部
206
第2復号部 (Dec2)
暗号化コンテンツ
207
再生部
モニタへ
スピーカへ
208
制御部
209
入力部
210
表示部
BDプレイヤ
200c
リモコンへ

【書類名】　要約書

【要約】

【課題】　再送要求による攻撃を回避することができる暗号送信装置及び暗号受信装置を提供する。

【解決手段】　サーバ装置は、コンテンツ鍵を５回暗号化して５個の暗号化コンテンツ鍵を生成し、コンテンツ鍵のハッシュ値を算出し、５個の暗号化コンテンツ鍵とハッシュ値とを送信する。映像再生装置は、５個の暗号化コンテンツ鍵とハッシュ値とを受信し、５個の暗号化コンテンツ鍵を復号してそれぞれコンテンツ鍵を生成し、生成したコンテンツ鍵のハッシュ値をそれぞれ算出し、算出したハッシュ値と受信したハッシュ値とを比較する。１組でも一致すれば、対応するコンテンツ鍵を正しいものとみなす。５組の全てで一致しなければ、復号エラーとみなす。

【選択図】　図３

特願２００３－１６７３７４

出願人履歴情報

識別番号 [０００００５８２１]

１．変更年月日 １９９０年 ８月２８日
[変更理由] 新規登録
住所 大阪府門真市大字門真１００６番地
氏名 松下電器産業株式会社